東北大学機関リポジトリ
TOUR
Tohoku University Repository
東北大学

# 不正アクセスの前兆検出機能を有する組織防衛型ネットワークセキュリティ管理システム



| | |
|---|---|
| 著者 | 根元　義章 |
| URL | http://hdl.handle.net/10097/41497 |

# 不正アクセスの前兆検出機能を有する
# 組織防衛型ネットワークセキュリティ管理システム

（課題番号　１２５５８０３６）

平成１２、１３年度科学研究費補助金（基盤研究(B)(２)一般）
研究成果報告書

東北大学図書
00031005618
附属図書館

平成１４年３月

研究代表者　根元　義章
（東北大学大学院情報科学研究科 教授）

# 平成 12、13 年度科学研究費補助金(基盤研究(B)(2)一般)
# 研究成果報告書

**研究課題**

不正アクセスの前兆検出機能を有する
組織防衛型ネットワークセキュリティ管理システム

**課題番号**

12558036

**研究組織**


研究代表者： 根元 義章 (東北大学大学院情報科学研究科教授)
研究分担者： 加藤 寧 (東北大学大学院情報科学研究科助教授)
曽根 秀昭 (情報シナジーセンター教授)
Glenn Mansfield ((株)サイバーソリューションズ代表取締役)


**研究経費**

平成 13 年度 4,700 千円
平成 14 年度 1,800 千円
計 6,500 千円

**研究発表**

1. **学会誌等**

[1] 金丸 朗, 太田 耕平, 加藤 寧, 根元 義章
**"マルチストレージ型分散トラヒックモニタリングシステムの提案と評価"**
電子情報通信学会論文誌, 条件付採録中, 2002

[2] 坂口 薫, 太田 耕平, 和泉 勇治, 加藤 寧, 根元 義章
**"2 次計画法に基づいたトラヒックパターンの比較による DDoS の追跡"**
電子情報通信学会論文誌, 条件付採録中, 2002

[3] 金丸 朗, 太田 耕平, 加藤 寧, 根元 義章
**"高速ネットワークに対応可能な DoS 攻撃の追跡技術—不正アクセスの抑制と根絶を目指して—"**
電子情報通信学会誌, Vol.84, No.10, pp.727-729, 2001.

[4] Pinai Linwong,Akihiro Fujii,Yoshiaki Nemoto
**"Buffer-Size Approximation for the Geo/D/1/K Queue"**
Networking ICN (International Conference on Networking) 2001.

[5] Shunsuke Nakamura, Kohei Ohta, Nei Kato, Yoshiaki Nemoto
**"A new scheme of combining advanced packet discard and dynamic bandwidth allocation for low delay/low jitter realtime communication using**

**CBQ/ALTQ"**

IEICE Trans. on Communication, Vol.E84-B, No.12, pp.3124-3132, 2001.

[6] 菅野浩徳，曽根秀昭，根元義章

**"デマンド型配送方式のネットニュースシステムへの適用と評価"**

情報処理学会論文誌，Vol.42，No.12，pp.2963-2972，2001.

[7] 武井 洋介，太田 耕平，加藤 寧，G. Mansfield，根元 義章

**"トラヒックパターンを用いた不正アクセス検出及び追跡方式"**

電子情報通信学会論文誌(B)，Vol.J84-B，No.8，pp.1464-1473，2001.

[8] Shunsuke Nakamura，Kohei Ohta，Nei Kato，Yoshiaki Nemoto

**"Proposal of Dynamic Bandwidth Allocation Technique for Low Delay/Low Jitter Realtime Communication and Its Evaluation by Using CBQ "**

IEICE Trans. on Communication, Vol.E84-B, No.6, pp. 1513-1520, 2001. .

[9] 金丸 朗，太田 耕平，加藤 寧，G. Mansfield，根元 義章

**"プロアクティブバッファリングを用いた高精度リモートトラヒック観測システムの提案と性能評価"**

電子情報通信学会論文誌(B)，Vol.J84-B，No.3，pp.392-401，2001.

[10] 真壁 知，太田 耕平，加藤 寧，G. Mansfield，根元 義章

**"ネットワークの負荷変動を考慮した動的なミラーサーバ選択方式"**

電子情報通信学会論文誌(B)，Vol.J84-B，No.3，pp.435-442，2001.

[11] Glenn Mansfield，Kohei Ohta，Yohsuke Takei，Nei Kato，Yoshiaki Nemoto

**"Towards Trapping Wily Intruders in the Large"**

COMPUTER NETWORKS 34，pp.659-670，2000.

[12] 加藤 寧，橋本 定，太田 耕平，根元 義章

**"管理情報の統合化によるネットワーク障害診断支援システムの提案と評価"**

電子情報通信学会論文誌(B)，Vol.J83-B，No.9，pp.1258-1266，2000.

[13] Akira Kanamaru，Kohei Ohta，Nei Kato，Glenn Mansfield，Yoshiaki Nemoto

**"A Simple packet aggregation technique for fault detection"**

International Journal of Network Management，Vol.10, No.4, pp.215-228, 2000.

[14] Kohei Ohta，Glenn Mansfield，Yohsuke Takei，Nei Kato，Yoshiaki Nemoto

**"Detection，Defense，and Tracking of Internet-Wide Illegal Access in a Distributed Manner"**

Proceedings of INET 2000.

[15] Kohei Ohta，Glenn Mansfield，Nei Kato，Yoshiaki Nemoto

**"Wide area fault detection by monitoring aggregated traffic"**

The First Passive and Active Mesurement Workshop，pp.25-31，2000.

[16] Pinai Linwong, Piya Tanthawichian, Akihiro Fujii, Yoshiaki Nemoto
**"Some New Results on the Geo/D/1/K Queueing System"**
TECHNICAL Proceedings of FOURTH INTERNATIONAL WORKSHOP ON QUEUEING NETWORKS WITH FINITE CAPACITY, 2000.

## 2. 招待講演

[17] 根元 義章
**"ネットワークの知的管理の実現に向けて"**
電子情報通信学会技術研究報告, CS2001-81, pp.55-64, 2001.

## 3. 研究会報告

[18] 坂口 薫, 太田 耕平, 和泉 勇治, 加藤 寧, 根元 義章
**"2 次計画法を用いたトラヒックパターンの比較による DoS の追跡手法の提案"**
電子情報通信学会技術研究報告, CS2001-89, pp.15-22, 2001.

[19] 油川 良太, 太田 耕平, 加藤 寧, 根元 義章
**"分散 NIDS による広域不正アクセスの検知手法の提案"**
電子情報通信学会技術研究報告, CS2001-80, pp.49-54, 2001.

[20] 角田 裕, 太田 耕平, 加藤 寧, 根元 義章
**"低軌道衛星ネットワークにおける TCP/IP 通信への TTL 情報 の利用法"**
電子情報通信学会技術研究報告, SAT2000-60, pp.33-44, 2000.

[21] 中村 俊輔, 太田 耕平, 加藤 寧, 根元 義章
**"CBQ を用いた動的帯域割当による実時間通信の提案と評価"**
電子情報通信学会技術研究報告, IN2000-50, pp.55-60, 2000.

[22] 真壁 知, 太田 耕平, 加藤 寧, Glenn Mansfield, 根元 義章
**"トラヒックの変化を考慮した動的なサーバ選択方法とその評価"**
電子情報通信学会技術研究報告, IN2000-95, pp.173-178, 2000.

[23] 菅野浩徳, 曽根秀昭, 根元義章
**"デマンド型ニュース配送方式におけるディレクトリサーバへのアクセス負荷低減手法"**
情報処理学会研究会報告, 分散システム/インターネット運用技術, 19-3, 2000.

[24] 角田 裕, 太田 耕平, 加藤 寧, 根元 義章
**"LEO 衛星ネットワーク向けハンドオーバを考慮した TCP の 輻輳制御に関する提案"**
電子情報通信学会技術研究報告, SAT2000-96, pp.81-86, 2000.

## 4. 口頭発表

[25] 宇津江 康太, 和泉 勇治, 太田 耕平, 加藤 寧, 根元 義章
**"passive/active な計測による動的なサーバ選択のコスト削減"**
2002 年電子情報通信学会総合大会, 印刷中

[26] 及川 達也, 太田 耕平, 加藤寧, 根元 義章
"統計的クラスタリング手法によるネットワーク状態の判別"
2002 年電子情報通信学会総合大会, 印刷中
[27] 坂口 薫, 和泉 勇治, 太田 耕平, 加藤 寧, 根元 義章
"2 次計画法を用いたトラヒックパターンの比較による DoS 攻撃の追跡"
2001 年電子情報通信学会総合大会, B-7-41, p.230, 2001.
[28] 宇津江 康太, 太田 耕平, 和泉 勇治, 加藤 寧, 根元 義章
"passive な情報を用いた AS 間の転送性能の推定に関する考察"
平成 13 年電気関係学会東北支部連合大会講演論文集, 講演番号 : 2H6
[29] 及川 達也, 太田 耕平, 加藤寧, 根元 義章
"パケット情報の関連付けによる DNS 障害発生原因の分類"
平成 13 年度電気関係学会東北支部連合大会講演論文集, 講演番号 : 2H12
[30] 金丸 朗, 太田 耕平, 加藤 寧, Glenn Mansfield, 根元 義章
"アドレス変換機能を有するパケットキャプチャシステムの設計と構築"
2000 年電子情報通信学会総合大会, B-7-36, p.129, 2000.
[31] 中村 俊輔, 太田 耕平, 加藤 寧, 根元 義章
"CBQ による IP ネットワーク上での実時間通信に関する一検討"
2000 年電子情報通信学会総合大会, B-7-79, p.172, 2000.
[32] 菅野 浩徳, 曽根 秀昭, 根元 義章
"ネットニュースにおけるデマンド型配送方式の提案"
2000 年電子情報通信学会総合大会, B-7-111, p.204, 2000.
[33] 真壁 知, 太田 耕平, 加藤 寧, Glenn Mansfield, 根元 義章
"トラヒックの観測情報を用いた動的なサーバ選択"
2000 年電子情報通信学会総合大会, B-7-138, p.231, 2000.
[34] 油川 良太, 太田 耕平, 加藤 寧, Glenn Mansfield, 根元 義章
"分散 NIDS と Access Tree を用いた広域不正アクセスの検出 方式の検討"
2000 年電子情報通信学会通信ソサイエティ大会, B-7-50, p.114, 2000.
[35] 真壁 知, 太田 耕平, 加藤 寧, Glenn Mansfield, 根元 義章
"スループットの変動環境における動的なサーバ選択"
2000 年電子情報通信学会通信ソサイエティ大会, B-7-50, p.114, 2000.
[36] 菅野 浩徳, 曽根 秀昭, 根元 義章
"マルチホーム環境における動的経路変更を考慮したサーバ選択手法"
平成 12 年度電気関係学会東北支部連合大会講演論文集, 2I25, p.349, 2000.

# 目次

# 不正アクセスの前兆検出機能を有する組織防衛型ネットワークセキュリティ管理システム

## 1. はじめに

インターネットの急速な発展に伴って、近年ネットワーク経由の不正アクセスが急増し、大きな社会問題となっている。インターネット経由の不正アクセスの代表例として、

(1)不正な手段を用いてアクセス権のないコンピュータ内に入り込み、機密情報の入手、システムの破壊または更なる不正アクセスの踏台にする不正侵入、

(2)発信者 IP アドレスを偽って、ターゲットに大量のトラヒックを集中させる Smurf 攻撃、

(3) WWW サーバや DNS(Domain Name System)サーバに大量な不完全接続を行い、接続数の上限を超えさせ、機能停止に追い込む DoS(Denial of Service)攻撃、

などがある。

利用者が安心してネットワークを使えるか否かは今後のインターネットの安定かつ健全な発展を占う重要な指標であり、ネットワークを不正アクセスから守る技術の研究開発は一刻を争う重要な課題である。

## 2. 不正アクセス検出に関する技術課題

不正アクセスを防止する方法として、これまで Firewall の利用や個々のコンピュータのソフトウエアバージョンアップを行うなどがある。しかし、Firewall は主要アプリケーションの防御ができず、バージョンアップ法は実施までにコストと時間を要する欠点があり、利用するには限界がある。多岐にわたる不正アクセスを効果的に防ぐには、不正アクセスが実行される前の共通的な特徴(以降前兆と呼ぶ)を捉えて、早期の段階で検出する必要がある。不正アクセスの前兆を検出し素早い対策を講じることにより、多岐に亘る不正アクセスに対処することが可能となる。しかし、一般的な運用ネットワーク上では、ユーザのトラヒックや管理用のトラヒックなど多種のトラヒックが混在しているため、不正アクセスの前兆を見つけるのは極めて困難であり、実現するには、綿密な事例検証に基づく新しいトラヒックの解析手法が必要となる。

## 3. 本研究の目的

本研究では、大規模運用ネットワークにおいて、トラヒックの観測および解析を行うことにより、不正アクセスに共通する前兆を発見できる新しい方式を提案し、これを基本とした不正アクセスの前兆検出・組織防衛型セキュリティ管理システムを構築することを目的とする。

## 4. 本研究の特色

これまでに開発された不正アクセス検出ツールはログ(ネットワーク利用歴)解析によるホスト監視型のものが多く、謂わば不正アクセスが起こったあとの事後処理の色彩が強い。少数ではあるが、リアルタイムでネットワークを監視し侵入を検出するツールもある。しかし、これらのツールはパターン照合型と言われるもので、ネットワーク上に流れるすべてのパケットの中身を抽出し、データベース上に蓄積されている「攻撃パターン文字列」(例：get passwd)と一致するか否かを検証する方式となっている。この手法は検出能力、監視可能な範囲、処理量などの点で限界がある。

これに対し、本研究で提案する前兆検出方式は従来のシステムの欠点を克服するものである。不正アクセスの前兆を捉えることによって、ルータでの遮断が可能になり、不正アクセスを未然に防ぐことができる。また、少量の投資で組織全体のネットワークを防衛する組織防衛型のネットワーク管理システムが実現でき、コストパフォーマンスの面で大変優れている。

## 5. 本研究の成果

本研究では、観測システムの構築を平成 12 年度に、検出システムの開発および検証実験を平成 13 年度にそれぞれ行った。以下、各年度における具体的な成果を述べる。

**平成 12 年度**

(1) 不正侵入、ネットワーク攻撃、サーバ攻撃などのネットワーク不正アクセスの特徴を分類し、それぞれの実行に必要な情報を整理した。不正アクセスの前兆となり得るパケットの種類や発生頻度などを明らかにし、これらの分類結果をもとにシステム全体の設計を行った。

(2) 東北学術ネットワーク TOPIC のインターチェンジセグメント上にトラヒ

ックをモニタリングするシステムを構築した。構築にあたり、トラヒックの最大瞬間速度、バースト特性などのネットワーク特性を考慮し、取りこぼしのないように観測間隔を決定した。

(3) 観測システムの構築後、実データの記録を開始し、実験データの採取を行った。データ採取はTCPのACK/RSTパケットなど不正アクセスの前兆に関連したものを中心に一ヵ月間行った。

**平成13年度**

(1) ping、scanなどの情報収集用ツールのソースおよび記録データを解析し、不正アクセスとその前兆の関係を明らかにした。さらに、不正アクセスの前兆を捉えるアルゴリズムを開発し、評価を行った。

(2) 不正アクセスの早期検出システムを開発した。具体的には、ネットワークプローブをデータ観測用に、ワークステーションをマネージャ用として用い、リアルタイムによる観測および検出システムを完成した。完成後、実際の運用ネットワークにおいて検出能力を実証し従来法との比較実験を行った。具体的には、検出件数の比較では、提案方法は従来法より2倍以上の検出能力を有することが判明した。また、検出のスピードでは、従来法より大幅に短縮できたことも確認した。

(3) 観測間隔と検出閾値などのパラメータの最適化を行い、組織防衛型のセキュリティシステムのプロトタイプを完成した。

(4)研究成果は学会などを通じ、広く公表を行った。

## 6. おわりに

ネットワークセキュリティシステムとして、これまでホスト監視型とネットワーク監視型の2つのタイプのものが存在していた。しかし、ホスト監視型では、ログの調査が基本であるため、不正アクセスの事後処理の色彩が強く、しかも、ログの改竄が意図的に行われた場合、根本的な対策となり得ない。一方、ネットワーク監視型では、データベースに蓄積されている既知の不正アクセスパターンとの照合による検出が基本であるため、ネットワークの通過パケットすべてを解析する必要があり、処理量の制限から小規模なLAN(10Mbps)にしか対応できない。さらに、不正アクセスパターンの変化に弱い欠点もある。

これらの既存方式に対し、本研究では、不正アクセスの前兆検出による組織防衛型のシステムを提案し、プロトタイプの構築により、運用ネットワークにおいてその有用性を検証した。提案システムは不正アクセスを未然に防げる点は従来のシステムにない大きな特徴である。また、提案システムは全パケットを見る必要がなく処理負荷が低いため、トラヒック量の大きいバックボーンネットワークにも適用でき、少量の投資で大きな効果が得られる長所もある。以上により本研究の目的は達成できたと言える。

# ABSTRACTS OF RESEARCH PROJECT, GRANT-IN-AID FOR SCIENTIFIC RESEARCH (2002)

1. RESERCH INSTITUTION NUMBER:11301
2. RESERCH INSTITUTION: Tohoku University
3. CATEGORY: Grand-in-Aid for Scientific Research (B)(2)
4. TERM OF PROJECT: (2000.4～2002.3)
5. PROJECT NUMBER: 12558036
6. TITLE OF PROJECT: Organization-defense Style Security System by using Detection of Omens of Illegal Access.
7. HEAD INVESTIGATOR: 60005527, Yoshiaki, Nemoto, Tohoku University, Graduate School of Information Sciences, Professor
8. INVESTIGATORS: (1) 00236168, Nei, Kato, Tohoku University, Graduate School of Information Sciences, Associate Professor
   (2) 40134019, Hideaki, Sone, Information Synergy Center, Professor
   (3) 99999999, Glenn, Mansfield, Cyber Solutions, Inc., President
9. SUMMARY OF RESEARCH RESULTS:

Along with the development of Internet, the detection of illegal access is becoming a major issue. A guarantee of a secure utilization of Internet is very vital for developers. Therefore, the technology of preventing Internet from intrusion and denial of service attacks is in great demand.

The typical cases of illegal access are as follows:

1- Penetrating and gaining privileges by illegal measures, then stealing classified information, destroying the system or using it as a stepping-stone for further attacks.
2- Forging the source IP address and sending a large amount of useless traffic.
3- Generating incomplete connections far beyond design limitations of the targeted WWW and DNS server to force it to no longer function.

In order to prevent illegal access, the detection of signs of an oncoming attack can be effective. By so doing, we can protect our network system beforehand.

In this research, we propose an organization-defense style security system by using the detection of omens (signs) of illegal access. This system detects various network scans that intend to find out vulnerability of remote network nodes. We implemented the system and evaluated its performance on an operating network. Experimental results show the effectiveness of our proposed system.

10. KEY WORDS

| | | |
|---|---|---|
| (1)Illegal Access | (2)Detection of Omens | (3)Security System |
| (4) | (5) | (6) |
| (7) | (8) | (9) |

11. REFERENCES


| AUTHORS, TITLE OF ARTICLE | JOUNAL, VOLUME-NUMBER, PAGES, YEAR |
|---|---|
| P. Linwong, **"Buffer-Size Approximation for the Geo/D/1/K Queue"** | Networking ICN 2001. |
| S. Nakamura, **"A new scheme of combining advanced packet discard and dynamic bandwidth allocation for low delay/low jitter realtime communication using CBQ/ALTQ"** | IEICE Trans. on Communication , Vol.E84-B, No.12, pp.3124-3132, 2001. |
| Y. Takei, **"Detecting and Tracing Iligal Access by using Traffic Patterns Matching Technique"** | IEICE Trans. on Communication , Vol.J84-B, No.8, pp.1464-1473, 2001. |
| S. Nakamura, **"Proposal of Dynamic Bandwidth Allocation Technique for Low Delay/Low Jitter Realtime Communication and Its Evaluation by Using CBQ "** | IEICE Trans. on Communication , Vol.E84-B, No.6, pp. 1513-1520, 2001. |
| A. Kanamaru, **"Proposal and Evaluation of Pro-active Buffering based Remote Monitoring System"** | IEICE Trans. on Communication , Vol.J84-B, No.3, pp.392-401, 2001. |
| S . Makabe , **" Dynamic Mirror Server Selection Method with Consideration about Fluctuation of Network Load"** | IEICE Trans. on Communication , Vol.J84-B, No.3, pp.435-442, 2001. |
| G. Mansfeild, **"Towards Trapping Wily Intruders in the Large "** | COMPUTER NETWORKS 34, pp.659-670, 2000. |
| N. Kato, **"A Proposal and Evaluation of Network Fault Management Supporting System by Intergrating Management Information"** | IEICE Trans. on Communication , Vol.J83-B, No.9, pp.1258-1266, 2000. |
| A. Kanamaru, **"A Simple packet aggregation technique for fault detection"** | International Journal of Network Management, Vol.10, No.4, pp.215-228, 2000. |
| K. Ohta, **"Detection, Defense, and Tracking of Internet-Wide Illegal Access in a Distributed Manner"** | Proceedings of INET 2000. |
| K. Ohta, **"Wide area fault detection by monitoring aggregated traffic"** | The First Passive and Active Measurement Workshop, pp.25-31, 2000. |
| P. Linwong, **"Some New Results on the Geo/D/1/K Queueing System"** | TECHNICAL Proceedings of FOURTH INTERNATIONAL WORKSHOP ON QUEUEING NETWORKS WITH FINITE CAPACITY, 2000. |

TOUR : Tohoku University Repository
コメント・シート

本報告書収録の学術雑誌等発表論文は本ファイルに登録しておりません。なお、このうち東北大学在籍の研究者の論文で、かつ、出版社等から著作権の許諾が得られた論文は、個別に TOUR に登録しております。

TOUR
http://ir.library.tohoku.ac.jp/